UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,913	12/29/2003	Jaroslaw Sydir	Intel-013PUS	1409

7590 04/07/2009

Daly, Crowley & Mofford, LLP
c/o PortfolioIP
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
04/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,913	SYDIR ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 3 to 20, 22 to 25, 27 to 32, 34-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3 to 20, 22 to 25, 27 to 32, 34-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/14/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 12/29/2003; amendment filed 1/8/2009.

2. Claims 1, 3 to 20, 22 to 25, 27 to 32, 34-41 are pending.

3. No new claim is added.

4. Claims 1, 3 to 20, 22 to 25, 27 to 32, 34-41 have been examined.

5. Claims 2, 21, 26, and 33 are cancelled.

Information Disclosure Statement

6. Information Disclosure Statement dated 11/14/2008 has been considered. Please see attached form PTO-1449.

Response to Arguments

7. After the interview held on November 12, 2008, Examiner called the applicant and informed him that after further consideration, Examiner's supervisor had found applicant's argument made during the interview non-persuasive.

8. With regards to claim 1, applicant argues that Ohta does not teach processing context each performing authentication. However, as indicated in the relevant part of the rejection, Ohta Paragraph [0012] teaches plural cipher processing units and paragraph [0046] teaches different cipher algorithms used to encrypt/decrypt the data. In showing the requirement of each processing context including authentication, the rejection states: "*paragraph [0046] and [0011] show that when a packet requires authentication and/or encryption, it will be routed to an authentication processing unit and/or encryption processing unit. Therefore, when a packet requires authentication, it will be assigned a processing context to perform authentication*". Therefore, the rejection clearly shows that the processing contexts of Ohta which require authentication, teach applicant's processing context.

Applicant further argues that the rejection does not teach the requirement of number of processing contexts not equal to authentication cores. In support of this argument, applicant cites a portion of the rejection and argues: "Since the claimed invention recites that "each processing context comprising authentication of the at least one packet" (emphasis added), the Examiner's assertion that a processing context may or may not require authentication is clear error." However, as indicated above, it is Ohta's processing contexts which require authentication, that teach applicant's processing context. The fact that Ohta teaches processing contexts of more variety does not

constitute an error in rejection. Ohta still teaches processing contexts that perform authentication.

Ohta's also teaches a number of processing contexts performing authentication different than the number of the authentication cores. As mentioned before, and in the rejections, Ohta teaches a variety of processing contexts. Claim requirement is that the processing context performs authentication of at least one packet. Let's call Ohta's processing context processing a first packet, the first processing context. The first packet requires authentication, and therefore the first processing context qualifies as applicant's processing context. Now, let's call Ohta's processing context processing a second packet, the second processing context. The second packet requires authentication and encryption, and therefore the second processing context also qualifies as applicant's processing context. Both first packet and the second packet are processed by Ohta's first authentication core, to perform the required authentication. Therefore, we have two processing contexts (first and second, which are different than one another) and only one authentication core. This meets all claimed requirements.

In addition, the rejection also mentions how Tardo teaches another scenario where the combination of Ohta and Tardo meets all claim requirements (see the last two lines of page 5 of the last office action). Applicant's argument relative to Tardo is that no specific portion of Tardo is cited to support the rejection. However, the cited portion of the

rejection clearly points out that Tardo teaches several authentication cores (see last paragraph of page 4 of last office action, and last sentence of the page 5 pointing to that portion in the relevant part of rejection). Applicant also argues that the rejection does not indicate how one of ordinary skilled in art would combine Ohta and Tardo, However, the last two sentence of page 5 and the first sentence of page 6 clearly shows how the one skilled in art would combine Ohta and Tardo and presents a motivation to do so.

Applicant further argues: "Moreover, for a portion of the claimed invention that recites "each buffer element corresponding to a respective one of the plurality of processing contexts," the Examiner states that "Figure 12 shows two buffer and two authentication processing units" (see page 5 of the Office Action). The Examiner's statement is not logical since the claimed invention recites "a number of the plurality of processing contexts does not equal a number of the authentication cores" and the Examiner is equating authentication processing units to processing contexts in his statement. Therefore, the Examiner has not shown that Ohta teaches each buffer element corresponding to a respective one of the plurality of processing contexts." However, it is not clear why Examiner's statement is not logical. Examiner shows an instance where each authentication processing unit (authentication core) get a corresponding buffer. As indicated before, processing contexts each have an authentication core performing the required authentication. Therefore, the buffer corresponding to the authentication processing unit (authentication core) also corresponds to the processing context (the

processing context that uses the authentication core). This clearly teaches each buffer element corresponding to a respective one of the plurality of processing contexts.

Applicant's argument relative to claims 10, 18, 25 and 32 is based on the same argument relative to claim 1, as discussed above.

With regards to claims 18, 25 and 32, applicant also argues that the limitation of an integrated circuit chip is not addressed. However, the rejection of claim 1 teaches a processor, and processors are implemented on integrated circuits (ICs). This is actually reflected in Ohta paragraph [0004] and also in Tardo column 3 lines 10-35. In addition, the implementation option of using ICs would have been known and obvious to the one skilled in art at the time of invention.

With regards to claims 36 to 38 applicant states again that examiner's rationale with respect to the authentication cores being unequal to processing contexts is illogical. However, as discussed above, Examiner's rationale perfectly teaches the claim requirement. Applicant also argues: "Also, the Examiner needs to specifically show for the record how Ohta teaches that the number of the plurality of processing contexts does not equal a number of the plurality of cipher cores since authentication cores are not the same as cipher cores." However, first, the Examiner has shown the above

requirement by the way of analogy. If applicant finds the analogy in error, applicant must show why. Merely stating that authentication cores are not the same as cipher cores is not a persuasive reason. If authentication cores were the same as cipher cores, there would be no analogy necessary, as the rejections would have been the same. A persuasive reasoning would show how the differences would make the analogy inapplicable.

Second, as shown in the above, the example processing contexts (first and second processing contexts) include a scenario where a processing context performs authentication and cipher processing (and therefore includes a cipher core), and a different processing context where the processing context performs authentication (and therefore could not includes a cipher core). Therefore, the number of cipher cores is unequal to number of processing contexts.

Applicant further argues: "Moreover, with respect to claims, 37, 39 and 41 the Examiner states that it would have been obvious to one of ordinary skill in the art that the number of the plurality of processing contexts is six, a number of the buffer elements is six, the number of the plurality of cipher cores is four and the number of the authentication cores is five. Applicants respectfully disagree. The Examiner has never shown how many processing contexts Ohta teaches much less that the number of processing contexts is different or even greater than the number of cipher cores and authentication

cores. In addition, the Examiners' assertion that Applicants' choice of quantities is merely an example is irrelevant statement and is not a basis for a proper rejection."

However, as indicated above, Ohta in view of Tardo teaches a scenario where the number of processing contexts is greater than the number of authentication cores (see example the first and second processing contexts detailed above).

In addition, in rejecting claims 37, 39, and 41, Examiner states that barring any unexpected results, it would have been obvious to the one skilled in art to have six processing contexts, with a buffer each, and four cipher cores, and five authentication cores. Note that the examples shown in the applicant's specification are just example scenarios, and no special feature or advantage is named with regards to those specific numbers for buffers, processing context, cipher cores, or authentication cores. Therefore, the statement clearly shows that the choice of numbers creates no unexpected result shown by the claim or applicant's specification, and therefore would be an obvious choice. Therefore, is the statement is not irrelevant and is a good basis for a proper rejection.

Based on the discussion above, applicant's argument relative to the allowability of the pending claims is non-persuasive. The rejections are maintained as follows.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 4-6, 8-20, 23-25, and 28-32, 36-41 are rejected under 35 U SC. 103(a) as being unpatentable over Ohta et al. (US 2002/0083317) hereinafter called Ohta, in view of Tardo (US 7,082,534)

10.1. Claims 1, 10, 13, 14, 15, 16, 18, 19, 20, 25, 32 disclose a processor, comprising: a crypto unit comprising:
a cipher core configured to cipher data received; (Ohta Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b))

a plurality of processing contexts each configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet (Paragraph [0012] teaches plural cipher processing units and paragraph [0046] teaches different cipher algorithms used to encrypt/decrypt the data. This would correspond to the "plurality of processing

contexts"), each processing context comprising authentication of the at least one packet (paragraph [0046] and [0011] show that when a packet requires authentication and/or encryption, it will be routed to an authentication processing unit and/or encryption processing unit. Therefore, when a packet requires authentication, it will be assigned a processing context to perform authentication);

Ohta teaches authentication cores configured to authenticate the ciphered data in Figure 12, Authentication Processing Unit 305a and 305b and associated text in paragraph [0104] Ohta does not teach but Tardo teaches, at least two authentications cores each implementing a different authentication algorithm as shown in Figures 2 and 3 and explained in column 4 lines 48-67 through column 5 lines 1-36. Figure 2 shows 2 authentication engines MD5 225 and SHA1 227. Figure 3 and associated text teach choosing the authentication engine based on the encryption as in column 5 lines 25-29. It would be obvious to one of ordinary skill in the art at the time of invention to use 2 different authentication algorithms of Tardo in two different authentication cores of Ohta. The motivation to combine would be that in paragraph [0046] of Ohta it states that the authentication algorithm includes HMAC-MD5-96 and HMAC-SHA-1-96. Therefore, as shown in Ohta the authentication cores include different algorithms); and

an authentication buffer configured to store the ciphered data and provide the ciphered data to the authentication cores each in an amount based on the corresponding authentication algorithm implemented. (Ohta Figure 12, Data Accumulation Unit 304a and 304b; paragraph [0011] states "a data block accumulation

unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authentication processing")

wherein the authentication buffer comprises buffer elements, each buffer element corresponding to a respective one of plurality of processing contexts (Figure 12 shows two buffers and two authentication processing units. Note also that as stated before, each packet requiring authentication will be stored (buffered) in a data accumulation unit until it is ready for encryption) and a number of plurality of processing contexts does not equal a number of authentication cores (processing contexts are comprised of a combination of authentication processing and/or encryption processes with the associated buffers, as shown in Ohta paragraph [0042]. Therefore, the system assigns a processing context for a packet, which may or may not require authentication. Therefore, the number of processing contexts is not equal to the number of authentication cores when a packet only requires encryption. Note also that as mentioned above, and according to Tardo's teachings, the system of Ohta in view of Tardo may include several authentication cores, each corresponding to a different authentication protocol, and therefore, the number of authentication cores may not be equal to number of processing contexts).

10.2. Claims 4, 23, 28 disclose the processor according to claim 1, wherein each of the buffer elements stores data for a respective one of the processing contexts (Ohta Figure 12 and associated text show a corresponding number of data block accumulation units to encryption processing units).

10.3. Claim 5 discloses the network processor according to claim 4, wherein the buffer elements have a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores (Ohta Figure 12, Data Accumulation Unit 304a and 304b; paragraph [0011] states "a data block accumulation unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authentication processing").

10.4. Claim 6 discloses the processor according to claim 1, wherein the crypto unit further comprises a plurality of cipher cores, and a plurality of authentication buffer elements (Ohta Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b)).

10.5. Claim 8 discloses the processor according to claim 6, wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks. (The rejection of claim one above and also, Ohta paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which would include all processor blocks in claims 8 and 9.)

10.6. Claim 9 discloses the network processor according to claim 8, wherein one of the cipher core cores processes data in 8-byte blocks and another one of the cipher cores

processes data in and/or 16-byte blocks. (The rejection of claim one above and also, Ohta paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which would include all processor blocks in claims 8 and 9.)

10.7. Claim 11 discloses the method according to claim 10, further comprising ciphering data received in a first one of a plurality of cipher cores to form the ciphered data (Ohta Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b).

10.8. Claim 12 discloses the method according to claim 10, further comprising ciphering data received using a first one of a plurality of cipher algorithms to form the ciphered data (Tardo Figure 2, DES 221 and AES 223).

10.9. Claims 17, 30, 31 disclose the method according to claim 10, further comprising determining whether data is to be ciphered (Ohta paragraph [0046], processing contexts).

10.10. Claims 24, 29 disclose the device according to claim 20, wherein the device includes one or more of a router, network switch, security gateway, storage area network client, and server (Ohta Paragraph [0089] teaches a router, firewall, and

security gate connecting plural computers. This is equivalent to the hardware devices mentioned in claims 20, 24, and 29).

10.11. Claim 36 discloses processor of claim 6 wherein the number of the plurality of processing contexts does not equal a number of the plurality of cipher cores (Ohta in view of Tardo teach the number of cipher cores unequal to the number of processing contexts the same way as it teaches the number of authentication cores unequal to processing contexts (see rejection of claim 1).

10.12. Limitation of claims 38 and 40 are substantially the same as claim 36.

10.13. Claim 37 discloses the processor of claim 36 wherein the number of the plurality of processing contexts is six, a number of the buffer elements is six, the number of the plurality of cipher cores is four and the number of the authentication cores is five (Ohta in view of Tardo teaches a system with a plurality of buffers, each corresponding to each processing context and a flexible number of authentication and cipher cores (not necessarily equal to the number of processing contexts, as discussed in claims 1 and 36). Therefore, barring any unexpected results, it would have been obvious to the one skilled in art to have six processing contexts, with a buffer each, and four cipher cores, and five authentication cores. Note that the examples shown in the applicant's specification are just example scenarios, and no special feature or advantage is named

with regards to those specific numbers for buffers, processing context, cipher cores, or authentication cores).

10.14. Requirements of claims 39 and 41 are substantially the same as claim 37.

11. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ohta et al. (US 200210083317) in view of Tardo (US 7,082,534), and further in view of Corder (US 7,069,447).

11.1. Ohta and Tardo teach claims 1 and 6 of the current application which claim 7 depends from as shown above. It however, does not teach a connection using a multiplexer device. Ohta teaches connections using a data path connection switching unit as in paragraph [0013].

Corder teaches authentication and encryption buffers and units connected with a multiplexer in column 7 lines 1-21.

Ohta in view of Tardo and Corder are analogous art, as they are directed to security systems performing encryption and authentication comprising processors and buffers connected via data paths. At the time of invention, it would have been obvious to use multiplexer devices as connection paths for connecting authentication and encryption buffers as taught by Corder to connect processors and buffers in Ohta in view of Tardo. The motivation to do so is providing various, flexible connection paths between elements, as suggested by Ohta paragraph [0129] , where it teaches that the

data path connection switching unit is used to provide various paths flexibly combined to fully take advantage of the multiple units. Therefore it would be obvious to one of ordinary skill in the art at the time of invention that this same inherent property of a multiplexer would be an alternate choice.

12. Claims 3, 22, 27, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohta et al. (US 2002/0083317) and Tardo (US 7,082,534), and further in view of "Speculation Techniques for Improving Load Related Instruction Scheduling", published in 1999, herein referred to as Spe.

12.1. Claims 3, 22, 27, 34, and 35 disclose the processor according to claim 1, wherein the plurality of processing contexts (Ohta Figure 12 and associated text show a corresponding number of data block accumulation units to encryption processing units).

Ohta in view of Tardo does not teach processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts.

Spe teaches processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of

processing contexts (Spe section 2.3 shows how downloading different portions of an execution program (packet data and key info as one portion, and processing of packet data as the other portion) into different pipelined banks hides the execution latency).

It would be obvious to one of ordinary skill in the art at the time of invention was made to use pipelining to hide the latency of data within the system of Ohta in view of Tardo, since Spe states at sections 1 and 2.3 that its method minimizes the stall time caused by waiting for missing data, for example the authentication buffer in Ohta.

Conclusion

13. **THIS ACTION IS MADE FINAL**. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

4/3/2009

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434